WE CLAIM:

1. A method for the secure distribution of digitised audio-visual works ("media") to consumers over a data network comprising the steps of:

encrypting said media using a different encryption key for each work ("media key"),

storing the encrypted media on one or more first servers,

storing the media keys on a second server,

making available one or more retail servers from which consumers may obtain the right to receive media keys for desired media in exchange for complying with conditions set by the retailer,

the consumer causing a request to be made from a network-connected client device to a selected retail server for at least the media key for a desired media work,

at the selected retail server, verifying the consumer has complied with the retailer's conditions, and if so,

the retail server either passing said request to the second server, or supplying to the client device data allowing the second server to be contacted,

at said second server verifying the allowability of fulfilling requests from said retail server or a client device and if so allowable encrypting the relevant media key and downloading it to either said retail server or said client device,

said retail server if receiving an encrypted media key from said second server, downloading said encrypted media key to said client device,

at the client device decrypting the received media key and storing it in memory,

at the client device generating a request to the appropriate first server to supply the desired media work,

from the first server downloading the desired encrypted media work downloading the encrypted media work to said client device, and

at the client device retrieving the media key from said memory and using it to decrypt the media work to a condition where it can be played using appropriate player software.

2. A method according to claim 1 wherein at the client device instead of decrypting the media key and storing it in memory the encrypted media key is stored in memory and when the encrypted media work is downloaded to said client device the encrypted media key is retrieved from memory, decrypted and used to decrypt the media work.

3. A method according to either of claims 1 or 2 including the steps of creating steering files corresponding to each media work and its corresponding key, said steering files containing information identifying the media work and the location of the media key, making available said steering files on said one or more retail servers, said steering files when processed on said client device causing a request to be made to said second server for the key for the media work identified in the steering file, said second server downloading said encrypted media key to said client device, and said client device generating a request to the first server to supply the encrypted media work identified in the steering file.

4. A method according to claim 3 wherein each steering file also contains information on the location of the corresponding media work and said steering file causes the client device to generate said request to the first server identified in said steering file to supply the encrypted media work.

5. A method according to either of claims 1 or 2 wherein said second server encrypts media keys for consumers using a public key encryption algorithm and when said client device generates a request to either said retail server or said second server for a media key it includes in the request the consumer's public key, said second server encrypting the relevant media key with the consumer's public key and upon receipt of said encrypted media key said client device decrypting the key using the consumer's private key.

6. A method as claimed in either of claims 1 or 2 wherein the client device stores the media key in volatile memory.

7. A method according to either of claims 1 or 2 wherein said retail server passes received client device requests to said second server and said second server upon verifying the allowability of fulfilling requests from said retail server downloading the encrypted media key to said retail server.

8. A method for the secure distribution of digitised audio-visual works ("media") to consumers over a data network comprising the steps of:
encrypting said media using a different encryption key for each work ("media key"),
storing the encrypted media on a first server,
storing the media keys on a second server,
making available a third server from which consumers may purchase media keys,
the consumer causing a request to be made from a network-connected client computer device to said third server for key for a desired media work,
the third server passing said request to the second server,
at said second server verifying the allowability of fulfilling said request and if so encrypting the relevant media key with a key unique to the consumer and downloading it to said third server,
said third server downloading said media key to said client device,
decrypting the media key at said client device and storing it in memory,
generating a request to the first server from said client device to deliver the desired media work,
delivering the encrypted media work from said first server to said client device,
retrieving the media key from said memory and using it to decrypt the media work to a condition where it is ready to play using appropriate player software.

9. A method for the secure distribution of digitised audio-visual works ("media") to consumers over a data network comprising the steps of:

encrypting said media using a different encryption key for each work ("media key"),

storing the encrypted media on a first server,

storing the media keys on a second server,

creating steering files corresponding to each media work and its corresponding key,

said steering files containing information identifying the media work and the location of the media key,

making available on a third server steering files corresponding to each media work for consumers to purchase,

said steering files when executed on a network-connected client device accessible to the consumer causing a request to be made to said second server for the key for the media work identified in the steering file,

at said second server verifying the allowability of fulfilling said request and if so encrypting the relevant media key with a key unique to the consumer and downloading it to said client device,

decrypting the media key at said client device and storing it in memory,

generating a request to the first server from said client device to deliver the media work identified in the steering file,

delivering the encrypted media work from said first server to said client device,

retrieving the media key from said memory and using it to decrypt the media work to a condition where it is ready to play using appropriate player software.

10. A method for the secure distribution of digitised products to consumers over a data network comprising the steps of:

encrypting said products using a different encryption key for each product ("product key"),

storing the encrypted product on a first server,

storing the product keys on a second server,

creating steering files corresponding to each product and its corresponding key,

said steering files containing information identifying the media work and the location of the product key,

making available on a third server steering files corresponding to each product for consumers to purchase,

said steering files when executed on a network-connected client computer device accessible to the consumer causing a request to be made to said second server for the key for the product identified in the steering file,

at the second server encrypting the relevant product key with a key unique to the consumer and downloading it to said client device,

decrypting the product key at said client device and storing it in memory,

generating a request to the first server from said client device to deliver the product identified in the steering file,

downloading the encrypted product from said first server to said client device,

retrieving the product key from said memory and using it to decrypt the product to a condition where it is ready for use.